REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-35 are pending.

5   **Specification Objection**

The Office objects to the underlined section headings throughout the specification (*Office Action* p.2). Appropriate amendments have been provided herein and Applicant respectfully requests that the specification objection be withdrawn.

10

35 U.S.C. §102 Claim Rejections

Claims 1-5, 7-12, 17-18, and 20 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,356,941 to Cohen (hereinafter, "Cohen") (*Office Action* p.3). Applicant respectfully traverses the rejection.
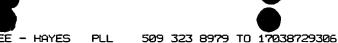
15

Claim 1 recites "initiating a request for accessing a dedicated data storage unit, the request specifying at least a remotely located secure storage facility containing the dedicated data storage unit and a user identification code, the secure storage facility associated with an address on a
20   communications network", and "identifying the dedicated data storage unit associated with the specified user identification code".

Cohen does not show or disclose a request specifying a remotely located secure storage facility and a user identification code, and identifying the dedicated data storage unit associated with the specified user identification
25   code, as recited in claim 1. Rather, Cohen describes a two-step process that includes a user logging onto a central storage facility (col.9, lines 5-6) and then the user logging onto a network vault to which access is desired (col.9, lines

21   *Docket No. 10990500-1*

23-24). Cohen states that a similar process for logging onto the central storage facility is preferably implemented to log onto the network vault (col.9, lines 25-26).

The Office relies on Cohen at col.2, lines 47-65; col.11, lines 54-58; col.12, lines 53-64; and col.13, lines 42-51 to reject the cited features of claim 1. However, Cohen only describes that a network vault enables data to be stored with controlled access by authorized user(s) (col.2, lines 53-55), and that a packet filter in a server verifies that packets are targeted only to the central storage facility (col.11, lines 54-58). There is no indication in these sections of Cohen that a dedicated data storage unit of a secure storage facility is associated with a specified user identification code which is specified in a request with an address to the secure storage facility to access the dedicated data storage unit, as recited in claim 1.

Further, Cohen describes that a lock manager may lock resources for execution such as a user identity for a transaction session (col.12, lines 53-60). However, there is no indication that the user identity for a transaction session is a user identification code specified in a request with an address to a secure storage facility and is associated with a dedicated data storage unit, as recited in claim 1. Cohen also describes that a security module determines whether a user has permission to access a network vault (col.13, lines 43-48). Again, there is no indication that a user permission to access a network vault is a user identification code specified in a request with an address to a secure storage facility and is associated with a dedicated data storage unit, as recited in claim 1.

Claim 1 also recites "in response to the request, automatically connecting to the remote secure storage facility at the associated address", Cohen also does not show or disclose automatically connecting to the remote

22

secure storage facility in response to a request for accessing a dedicated data storage unit, as recited in claim 1. The Office relies on Cohen at col.4, lines 23-45 which describes that a user is provided access to a network vault if permitted to do so. However, there is no indication of automatically

5   connecting to a remote secure storage facility in response to a request specifying at least a remotely located secure storage facility containing the dedicated data storage unit and a user identification code, as recited in claim 1.

Accordingly, for these reasons, claim 1 is allowable over Cohen and Applicant respectfully requests that the §102 rejection be withdrawn.

10

Claims 2-5 and 7-12 are allowable by virtue of their dependency upon claim 1 (either directly or indirectly). Additionally, some or all of claims 2-5 and 7-12 are allowable over Cohen for independent reasons. For example:

Claim 2 recites that "granting access includes granting access to the

15   identified dedicated storage unit in accordance with pre-existing instructions associated with the specified user identification code." Cohen does not show or disclose pre-existing instructions associated with a specified user identification code, as recited in claim 2.

The Office relies on Cohen at col.9, lines 1-22 which describes that a

20   user logs onto a central storage facility via client software with identifiers. However, there is no indication of instructions associated with the specified user identification code, as recited in claim 2, and the Office has not provided an indication as to which specific feature of Cohen is being relied upon to reject claim 2. Accordingly, Applicant respectfully requests that the Office

25   withdraw the §102 rejection of claim 2.

Claim 3 recites that "the request further specifies a processor identification code associated with a client computer, the step of identifying the

Docket No. 10990500-1

dedicated data storage unit including identifying the dedicated data storage unit associated with both the specified user identification code and the specified processor identification code." Cohen does not show or disclose a processor identification code associated with a client computer, that the request specifies

5 the processor identification code, or identifying a dedicated data storage unit associated with both the specified user identification code and the specified processor identification code, as recited in claim 3.

The Office relies on Cohen at col.4, lines 45-60; and col.9, lines 29-31 which describes a user logging onto a network vault by providing an identifier

10 to the network vault (col.4, lines 52-54) and that user identification and authentication must at least be performed before access is granted to any network vault (col.9, lines 29-31). There is no indication in Cohen of a processor identification code or of identifying a dedicated storage unit associated with both a user identification code and a processor identification

15 code. Accordingly, Applicant respectfully requests that the Office withdraw the §102 rejection of claim 3.

Claim 7 recites that "the request further specifies at least one data file stored on the identified dedicated data storage unit." Cohen does not show or disclose that the request specifies a remotely located secure storage facility

20 containing the dedicated data storage unit and a user identification code (claim 1) in combination with a data file stored on the identified dedicated data storage unit, as recited in claim 7.

The Office relies on Cohen at col.3, lines 53-64 which describes that the data is a collection of files which are only accessible through a filing system.

25 However, there is no indication of a request that specifies the combination of features recited in claims 1 and 7. Accordingly, Applicant respectfully requests that the Office withdraw the §102 rejection of claim 7.

24 *Docket No. 10990500-1*

Claim 17 recites a secure storage facility comprising "one or more dedicated data storage units for storing data files in a secure environment, each of the dedicated data storage units identified by at least one user identification

5   code", and means for "identifying a dedicated data storage unit associated with the specified user identification code" and "granting access to the identified dedicated data storage unit in accordance with a set of instructions associated with the specified user identification code."

Cohen does not show or disclose a dedicated storage unit identified by a

10   user identification code, or identifying a dedicated data storage unit associated with the specified user identification code, as recited in claim 17. The Office rejects claim 17 based on the discussion of claim 1 (*Office Action* p.7), where the Office relies on Cohen at col.2, lines 47-65 and col.11, lines 54-58. However, Cohen only describes that a network vault enables data to be stored

15   with controlled access by authorized user(s) (col.2, lines 53-55), and that a packet filter in a server verifies that packets are targeted only to the central storage facility (col.11, lines 54-58). There is no indication in Cohen that a dedicated data storage unit is associated with a user identification code, as recited in claim 17.

20   Cohen also does not show or disclose granting access to the identified dedicated data storage unit in accordance with a set of instructions associated with the specified user identification code, as recited in claim 17. As described above, the Office rejects claim 17 based on the discussion of claim 1, but claim 1 does not recite any such feature. Claim 2 recites a similar feature and

25   the Office relies on Cohen at col.9, lines 1-22 which describes that a user logs onto a central storage facility via client software with only identifiers.

25   *Docket No. 10990500-1*

However, there is no indication of instructions associated with the specified user identification code, as recited in claim 17.

Accordingly, claim 17 is allowable over Cohen and Applicant respectfully requests that the §102 rejection be withdrawn.

5

Claims 18 and 20 are allowable by virtue of their dependency upon claim 17. Additionally, claims 18 and/or 20 are allowable over Cohen for independent reasons. For example:

Claim 20 recites that "the set of instructions associated with a user
10 identification code specifies read-only, write-only or read/write access to data files stored in the dedicated data storage unit associated with that user identification code." Cohen does not show or disclose these specific data file instructions associated with the user identification code. The Office relies on Cohen at col.14, lines 46-65 to reject claim 20. However, there is no indication
15 in Cohen of the specific data file instructions recited in claim 20, and the Office has not provided an indication as to which specific features of Cohen are being relied upon to reject claim 20. Accordingly, Applicant respectfully requests that the Office withdraw the §102 rejection of claim 20.

20 **35 U.S.C. §103 Claim Rejections**

A. Claims 6 and 19 are rejected under 35 U.S.C. §103(a) for obviousness over Cohen in view of U.S. Patent No. 5,671,285 to Newman (hereinafter, "Newman") (*Office Action* p.8). Applicant respectfully traverses the rejection.

25 **B.** Claims 13-16 are rejected under 35 U.S.C. §103(a) for obviousness over Cohen in view of U.S. Patent No. 6,067,618 to Weber

26

Docket No. 10990500-1

(hereinafter, "Weber") (*Office Action* p.9). Applicant respectfully traverses the rejection.

<u>Claim 6</u> is dependent upon claim 1 and recites that "each data file stored
5   in the dedicated data storage unit has a predetermined security level assigned
thereto, each data file being encrypted in accordance with its assigned security
level." Cohen and/or Newman do not teach or suggest a data file having a
predetermined security level assigned thereto and the data file being encrypted
in accordance with the assigned security level, as recited in claim 6. Further,
10   Newman describes encrypted transmission of information during a
communication and is not relevant to encrypted data storage as claimed in the
present application.

The Office recognizes that Cohen does not teach a data file having a
predetermined security level assigned thereto, and the data file being encrypted
15   in accordance with the assigned security level (*Office Action* p.8). The Office
relies on Newman at col.5, lines 30-45; col.6, lines 20-30; col.11 lines 34-43;
and col.15, lines 17-32 to reject claim 6. However, Newman only describes
that a facsimile terminal unit contains a unique private code which may be
randomly generated and public keys (col.5, lines 30-45), and that a fax terminal
20   offers a variety of communications modes which may include a level of
security (col.6, lines 9-30). There is no indication in these sections of Newman
of a data file being encrypted and stored according to an assigned security
level, as recited in claim 6.

Newman also describes that secure FAX pages can be sent and billed
25   based on their levels of security (col.11, lines 34-43), and Newman claim 11
recites that a message is transmitted according to a selected level of security
(col.15, lines 17-32). Again, there is no indication in these sections of

27   *Docket No. 10990500-1*

Newman of a data file being encrypted and stored according to an assigned security level, as recited in claim 6.

Accordingly, claim 6 is allowable over the Cohen-Newman combination and Applicant respectfully requests that the §103 rejection be withdrawn.

5

Claim 19 is dependent upon claim 18 and recites "a data file to be stored in the dedicated data storage unit associated with a user identification code is encrypted in accordance with a user assigned security level." Claim 19 is rejected over the Cohen-Newman combination for the same reasons as claim 6.

10 As described above in the response to the rejection of claim 6, there is no indication in Newman of a data file being stored and encrypted in accordance with a user assigned security level, as recited in claim 19.

Accordingly, claim 19 is allowable over the Cohen-Newman combination and Applicant respectfully requests that the §103 rejection be

15 withdrawn.

Claim 13 recites a "remote secure storage facility identified by an address on the communications network and including at least one dedicated data storage unit for storing data files associated with a user identification

20 code", "the remote secure storage facility adapted to allow access to the at least one dedicated data storage unit in accordance with a set of pre-existing instructions". Claim 13 is rejected over the Cohen-Weber combination for the same reasons as claims 1-5, 7, and 10-12.

As described above in the response to the rejection of claim 1, Cohen

25 does not teach or suggest a dedicated data storage unit for storing data files associated with a user identification code, as recited in claim 13. Cohen only describes that a network vault enables data to be stored with controlled access

28

by authorized user(s) (col.2, lines 53-55), and that a packet filter in a server verifies that packets are targeted only to the central storage facility (col.11, lines 54-58). There is no indication that a dedicated data storage unit is associated with a user identification code.

5   Further, As described above in the response to the rejection of claim 2, Cohen does not teach or suggest allowing access to a dedicated data storage unit in accordance with a set of pre-existing instructions, as recited in claim 13. Cohen only describes that a user logs onto a central storage facility via client software with identifiers (col.9, lines 1-22). There is no indication of

10   instructions or of a secure storage facility adapted to allow access to a dedicated data storage unit in accordance with a set of pre-existing instructions, as recited in claim 13.

Claim 13 also recites "receiving a request from a user on the client computer to access the logical data storage peripheral, the request specifying at

15   least the logical data storage peripheral and a user identification code", and "automatically connecting to the remote secure storage facility".

As described above in the response to the rejection of claim 1, Cohen does not teach or suggest a request specifying a logical data storage peripheral and a user identification code, as recited in claim 13. Rather, Cohen describes

20   a two-step process that includes a user logging onto a central storage facility (col.9, lines 5-6) and then the user logging onto a network vault to which access is desired (col.9, lines 23-24). Cohen states that a similar process for logging onto the central storage facility is preferably implemented to log onto the network vault (col.9, lines 25-26).

25   Further, as described above in the response to the rejection of claim 1, Cohen does not teach or suggest automatically connecting to the remote secure storage facility, as recited in claim 13. Cohen only describes that a user is

Docket No. 10990500-1

provided access to a network vault if permitted to do so (col.4, lines 23-45). There is no indication of automatically connecting to a remote secure storage facility in response to a request, as recited in claim 13.

Weber is not cited by the Office for describing any of these features of
5   claim 13. Accordingly, for these reasons, claim 13 along with dependent claims 14-16 are allowable over the Cohen-Weber combination and Applicant respectfully requests that the §103 rejection be withdrawn.

New Claims

10   New claims 21-35 are presented for examination. Based on the above discussion regarding Cohen, the Cohen-Newman combination, and the Cohen-Weber combination, Applicant believes that claims 21-35 are also allowable.

15   ### Conclusion

Pending claims 1-35 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. If any issues remain that preclude issuance of this application, the Examiner is urged to contact the undersigned attorney before issuing a subsequent Action.

20

Respectfully Submitted,

Dated: Dec 31, 2003   By: _David A. Morasch_
25   David A. Morasch
                                     Reg. No. 42,905
                                     (509) 324-9256 x 210

30